WHAT IS CLAIMED IS:

1. In a computer-implemented trust management system, a method for controlling access to a computing resource, the method including:

obtaining a request for the computing resource;

obtaining a group of certificates, each certificate expressing at least one authorization by at least one principal;

identifying a set of principals associated with the certificates;

initializing a state associated with each principal;

evaluating a certificate as a function, at least in part, of the state associated with one or more of the principals;

updating the state of one or more of the principals if the result of said evaluating step indicates that the state of a principal should be changed; and

repeating said evaluating and updating steps until a fixpoint is reached or until a predefined principal is found to authorize the request.

2. A method as in claim 1, further including:

constructing a dependency graph, the dependency graph containing a node corresponding to each principal in the set of principals; and

connecting at least two nodes in the dependency graph with a certificate that expresses a dependency of one node on the state of another node;

wherein the dependency graph is used, at least in part, during said evaluating, updating, and repeating steps to determine which certificates to evaluate.

3. A method as in claim 1, in which said updating step is performed after all of the certificates have been evaluated.

4. A method as in claim 1, in which the request for the computing resource is obtained from a first principal, and in which at least one of the certificates is obtained from the first principal, the certificate having been issued by a second principal.

5. A method as in claim 1, in which the certificates comprise Simple Public Key Infrastructure certificates.

6. A method as in claim 1, in which the computing resource is one of: access to a piece of electronic content; use of a computer program; ability to execute a transaction; access to a computer; and access to a network.

7. A computer program product for making trust management determinations, the computer program product including:

computer code for obtaining a request to perform a predefined action;

computer code for obtaining a group of authorizations for the predefined action, one or more of the authorizations in the group being a function of the authorization state of one or more principals;

computer code for identifying a set of principals associated with the authorizations and for initializing a state associated with each principal;

computer code for evaluating authorizations from the set of authorizations using the state associated with each principal;

computer code for updating the state of the principals;

computer code for causing repeated execution of said computer code for evaluating authorizations and for updating the state of the principals until a fixpoint is reached or until a predefined principal is deemed to authorize the request; and

a computer-readable medium for storing the computer codes.

8. A computer program product as in claim 7, in which the computer readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, network server, hard drive, optical storage, and a data signal embodied in a carrier wave.

9. A system for controlling access to electronic content or processing resources, the system comprising:

means for receiving a request from a requesting principal to access a piece of electronic content or a processing resource;

means for collecting a set of one or more certificates relating to the request, the requesting principal, or the electronic content or processing resource;

means for identifying a root principal from whom authorization is needed in order to grant the request;

means for performing at least a portion of a least fixpoint computation over said certificates to determine whether the root principal has authorized the requesting principal to access the piece of electronic content or processing resource; and

means for granting access to the electronic content or processing resource if the least fixpoint computation indicates that the root principal has authorized said access.

10. A system for controlling access to electronic resources, the system comprising:

a first computer system for processing requests for system resources, the first computer system comprising:

a network interface for receiving digital certificates from other systems and for receiving requests to access electronic resources;

a memory for storing electronic resources and one or more certificates relating thereto; and

a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by performing least fixpoint computations using said digital certificates.

11. A system as in claim 10, further comprising:

a second computer system for making a request for system resources from the first computer system;

a third computer system for generating a first digital certificate, the first digital certificate authorizing, at least in part, the second computer system to access a predefined system resource;

12. A system as in claim 11, further comprising:

a fourth computer system, the fourth computer system being operable to generate a second digital certificate, the second digital certificate

authorizing, at least in part, the third computer system to authorize, at least in part, the user of the second computer system to access the predefined system resource.

13. A system as in claim 12, in which the third computer system is operable to send the first digital certificate to the second computer system, the second computer system is operable to send the first digital certificate to the first computer system in connection with said request, and the fourth computer system is operable to send the second digital certificate to the first computer system.

14. A system as in claim 13, in which the first computer system further comprises a public key associated with the fourth computer system, the public key corresponding to a private key used to sign the second digital certificate.

15. A system as in claim 10, in which at least some of the digital certificates comprise SPKI certificates.

16. A system as in claim 10, in which at least some of the digital certificates comprise Keynote certificates.

17. A method for performing trust management computations, the method including:

collecting a group of certificates, each certificate including at least one authorization;

expressing authorizations using a structure that satisfies certain predefined properties;

expressing each certificate as a function, wherein each function possesses one or more properties sufficient to ensure that a set of authorizations will have a fixpoint;

computing a fixpoint of the authorizations, or an approximation thereof;

making a trust management decision using the result of said computing step.

18. A method as in 17, in which the structure comprises a lattice.

19. A method as in claim 17, in which the structure is chosen such that it provides an ordering for authorizations, a way to combine authorizations, and a way to express certificates as monotone functions.

20. A method as in claim 18, in which the one or more properties sufficient to ensure that a set of authorizations will have a fixpoint includes the property that each function is monotone.